UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,568	04/11/2006	**Dirk Gandolph**	PD030108	1348

24498 7590 03/24/2009
Robert D. Shedd
Thomson Licensing LLC
PO Box 5312
PRINCETON, NJ 08543-5312

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
03/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/575,568	**Applicant(s)** GANDOLPH ET AL.
	Examiner JEFFREY D. POPHAM	**Art Unit** 2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-8 and 10-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-8 and 10-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Remarks

Claims 1-4, 6-8, and 10-12 are pending.

Response to Arguments

1. Applicant's arguments filed 1/8/2009 have been fully considered but they are not persuasive.

Applicant argues that support for the amendment, including "wherein the second decryption key is not used for decrypting the first data set" is found in the application as originally filed, such as page 10, lines 21-26 and page 12, lines 27-30. The passage on page 10 describes encryption keys and not decryption keys. This paragraph refers to first and second keys and that they are to be used as in the seventh embodiment, which is described in the 2 immediately paragraphs. This description makes it clear that 2 encryption keys are used for encrypting sets of data, however, a single decryption key (K3) is used for decrypting data that was encrypted by either of the encryption keys. Therefore, only a single decryption key is disclosed, while multiple encryption keys may be used. The paragraph referred to on page 12 merely discusses that a removable storage device may hold more than one decryption key, "wherein at least one key may be used for decryption of supplementary data". This does not distinguish a first and second decryption key as claimed, but merely states that at least one of the stored keys (which may be the same key as that used to decrypt a first set of data stored on the medium) may be used for decryption of supplementary data. While the application as originally filed appears to have broad support for use of multiple decryption keys (as is shown in the section cited on page 12), there is no support in the application as originally filed for the limitation "wherein the second decryption key is not used for decrypting the first data set."

Applicant argues that Kelly teaches that both the disk key and title key must be used together to decrypt the basic content, i.e. the first data set and, therefore, does not teach that the second decryption key is not used for decrypting the first data set. There are various Interpretations, however, in which this is not the case. For example, the first data set may be the title keys themselves, that are decrypted by use of the disk key. Paragraph 51 of Kelly describes that the additional content items downloaded from the server may be protected by use of "the ACC, the disc key or the title keys." One will see from this paragraph that the downloaded content (which can be seen as the second data set of claim 1, for example) may be decrypted with the title keys, which were not used in decrypting of the first data (the first data set being the title keys themselves). In another interpretation, the first data set may be the content stored on the disk. In this situation, the title keys are used for decrypting the content/first data set. As noted in paragraph 51 above, 3 separate entities may be used for protection of the additional content downloaded from the server. In this case, the disk key may be used for decrypting the additional content, which corresponds to the second data set. One can see that the content stored on the disk can be decrypted with the title keys, while the additional content downloaded from the server can be decrypted with the disk key. Paragraphs 63-64, for example, further describe these situations, in that a session key for encrypting the additional content from the server is the encrypted disk key and that the encryption can be made with the disk key or title key.

However, in order to explicitly show a separate key that is solely used for decryption of data from a second data source, new grounds of rejection have been provided.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 1-4, 6-8, and 10-12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The independent claims have been amended to provide for 2 keys, one used for decrypting the first set of data, and the other being used for decrypting the second set of data, "wherein the second decryption key is not used for decrypting the first data set." There is no basis for this amendment in the application as originally filed. As described above in the response to arguments, while the application as originally filed broadly discusses multiple decryption keys, there is no basis for the limitation "wherein the second decryption key is not used for decrypting the first data set" as claimed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 6, 8, 11, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly (U.S. Patent Application Publication 2003/0072453) in view of Newton (U.S. Patent 5,771,291).

Regarding Claim 1,

> Kelly discloses method for decrypting data within a device, the data comprising an encrypted first data set and an encrypted second data set, wherein the first data set and at least two respective device independent electronic decryption keys are stored on a removable prerecorded storage medium (Abstract; and Paragraphs 31-34, 51, and 63-64), and the second data set is not stored on the removable prerecorded storage medium but is related to the first data set (Abstract; and Paragraph 30, the method comprising the steps of:

Retrieving the first data set and the device independent decryption keys from the removable storage medium (Abstract; and Paragraphs 34-35);

Retrieving the second data set from a second data source (Abstract; and Paragraphs 50 and 57);

Decrypting the first data set using a first of the decryption keys (Abstract; and Paragraphs 36 and 44); and

Decrypting the second data set using a second of the decryption keys, wherein the second decryption key is not used for decrypting the first data set (Abstract; and Paragraphs 50-52, 58-59, and 63-64);

But does not explicitly disclose that the second decryption key is distinct from all keys used for decrypting data on the storage medium (though this is not precisely claimed, it appears to be what Applicant wishes the scope of the claims to be and is rejected herein for completeness).

Newton, however, discloses decrypting a second data set, retrieved from a second data source, using a decryption key that is stored on the removable prerecorded storage medium, wherein the decryption key is not used for decrypting any data on the storage medium (Column 9, lines 33-44). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication system of Newton into the secure content distribution system of Kelly in order to allow the system to verify that the user is authentic as well as the medium, thereby providing an additional level of protection such that, even if the medium were to be stolen, it would be un-usable without the user's password.

Regarding Claim 6,

Claim 6 is an apparatus claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 3,

Kelly as modified by Newton discloses the method of claim 1, in addition, Kelly discloses a step of detecting whether the removable storage medium and the second data set are authorized by the same authority, wherein the second data set is regarded as authorized if it can be decrypted by the second decryption key (Abstract; and Paragraphs 50-52, 58-59, and 63-64).

Regarding Claim 11,

Claim 11 is an apparatus claim that is broader than method claim 3 and is rejected for the same reasons.

Regarding Claim 8,

Kelly as modified by Newton discloses the method of claim 1, in addition, Kelly discloses that the first electronic decryption key is the only suitable key for decrypting the first data set, and the second decryption key is one of several suitable keys for decrypting the second data set (Abstract; and Paragraphs 36, 44, 51, 58-59, and 63-64).

Regarding Claim 12,

Claim 12 is an apparatus claim that corresponds to method claim 8 and is rejected for the same reasons.

4. Claims 2 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of Newton, further in view of Getsin (U.S. Patent 6,529,949).

Regarding Claim 2,

Kelly as modified by Newton does not explicitly disclose a step of determining from a plurality of data sets on the second data source a second data set that refers to the removable storage medium, wherein the data set refers to different removable prerecorded storage media.

Getsin, however, discloses a step of determining from a plurality of data sets on the second data source a second data set that refers to the removable storage medium, wherein the data set refers to different removable prerecorded storage media (Column 27, line 56 to Column 29, line 4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the remote playback control system of Getsin into the secure content distribution system of Kelly as modified by Newton in order to provide supplemental data for a plurality of media (e.g.

DVDs) on a server, allowing clients to access only the data directed to the media for which the client currently has access to (such as being played), while ensuring authentication and authorization of the user, client, and/or DVD before allowing access to such supplemental data, and/or to allow the system to access supplemental data held on the currently playing DVD via such authentication and authorization processing.

Regarding Claim 7,

Claim 7 is an apparatus claim that corresponds to method claim 2 and is rejected for the same reasons.

5. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of Newton, further in view of Qawami (U.S. Patent Application Publication 2002/0176575).

Kelly as modified by Newton does not explicitly disclose that the electronic decryption keys are only accessible while a removable prerecorded storage medium that contains the electronic decryption keys is readable.

Qawami, however, discloses that the electronic decryption keys are only accessible while a removable prerecorded storage medium that contains the electronic decryption keys is readable (Paragraphs 38, 42, 44, 54-58, and 94). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key protection techniques of Qawami into the secure content distribution system of Kelly as modified by Newton in order to only provide access of keys while the keys are being used to decrypt specific data on the disk, and to delete the keys immediately after use, thereby only storing the keys for the amount of time it takes to decrypt the data, and/or to never store particular keys used for decryption on the device, such that security of the keys is increased by ensuring that exposure to such keys is kept to a minimum.

6. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of Newton, further in view of Schneier (Schneier, Bruce, “Applied Cryptography”, Second Edition, 1996, pp. 1-14).

Kelley as modified by Newton does not explicitly disclose that the first and second data sets are encrypted using RSA coding.

Schneier, however, discloses that the first and second data sets are encrypted using RSA coding (Pages 6-14). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the encryption algorithm of Schneier into the secure content distribution system of Kelly as modified by Newton in order to use an encryption algorithm that is well known, easy to understand and implement, widely used, and secure in that it has not been broken.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437